Reference No.: ____________

CONFIDENTIAL

Who? Vision Systems, Inc.

RECORD OF INVENTION
AND INVENTION DISCLOSURE

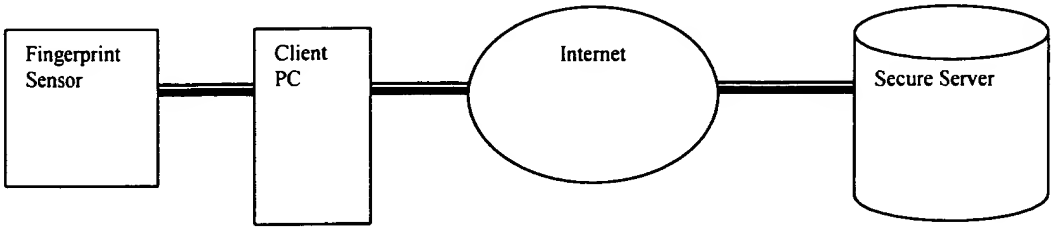
1. Title of Invention: **Server side storage and protection of private cryptographic keys**

2. Inventor(s):

Full Name* (Including middle initial)	Citizenship	City, State & Country of Residence	Postal Address (where mail is received)
Alex Dickinson	Australia	Laguna, CA, USA	

3. Conception of the Invention:

4. Initial Drawings or Sketches and Written Description of the Invention:



5. Initial Disclosure of the Invention to Others:

Date	Place	Person(s) Receiving Disclosure	Circumstances
7/30/99	Who? Vision Systems, Inc.	Brian Berger	

6. Initial Tests, Uses or Operations of the Invention:

7.

8.

9.

10.

11.

12.

(2) DESCRIPTION. Write a detailed description of the invention, referencing sketches drawings or photographs. Describe the best way to carry out the invention.

In this invention, we suggest an alternative scheme that does not rely on the user's ability to protect the secret key in anyway. In this scheme the private key is stored within a secured server. And associated with a biometric template pertaining to the owner of the private key. The server is configured to meet the following requirements.

1. Under absolutely no conditions may the private key leave the server.
2. The private key may only be accessed upon presentation of an incoming biometric template that matches the stored template.
3. Upon matching, the private key may be only used to enable a limited set of standard cryptographic operations such as digital signatures and encryption.

Implementation

This scheme may be implemented within a standard computer structure or if a higher level of security is desired the secret key and biometric maybe stored within a dedicated piece of hardware associated with the server. A simple example, of the later, would be a large bank of smart cards each containing the biometric template, private key and a cryptographic engine. In such a configuration, neither the biometric or secret key would need to leave the confines of the smart card.

Note that it is also critical to guard the security of the incoming biometric template. Two means are listed as follows:

1. At the point of acquisition of the biometric template e.g. the Biometric sensor. The template is encrypted at the server. This insures that only the secure server that is in possession of the matching private key may encrypt the template.
2. At the point of acquisition of the biometric template e.g. the Biometric sensor. The template is encrypted at the server. With the public key of the user. This insures that only the template may only be decrypted given access to the users private key, which may in fact be stored with the bank of smart cards, refereed to above. This scheme insures that even if the server's private key is compromised, the biometric templates will remain secure.

(3)

13.